Course Code	Course Name				
MCAE342	Digital Forensics				
Teaching Scheme: Contact Hours (Per Week)			Credits Assigned		
Theory	Tutorial	Total	Theory	Tutorial	Total
3	1	4	3	1	4
Examination Scheme (Marks)					
Internal Assessment (IA)			End Sem. Examination	Term Work	Total (Marks)
Continuous Assessment CA)	Test	Total (IA) (CA+Test)			
25	25	50	50	25	125

Pre-requisite: Knowledge of Internet, Computer Network , Cyber security

Course Objectives: Course aim to

Sr. No.	Course Objective
1	Understand the fundamental concepts, types, and impact of cybercrime, Learn the principles and the role of digital evidence in of digital forensics investigations.
2	Learn methodologies for identifying, containing, and mitigating cyber incidents and Understand the legal, ethical, and procedural aspects of digital forensic investigations
3	Learn forensic data acquisition techniques and duplication methods
4	Investigate and interpret forensic artifacts in Windows operating systems. Explore volatile and non-volatile memory sources in forensic investigations
5	Understand techniques for investigating network-based attacks and intrusions Learn Mobile Forensic Techniques
6	To explore the techniques used in Email Forensic and Internet Artifacts analysis.

Course Outcomes (CO): On successful completion of course learner/student will be able to

Sr.No.	Course Outcome	Bloom Level
CO1	Define cybercrime and its categories, Identify the key concepts of digital forensics, List various types of digital evidence	Remembering
CO2	Describe the phases of an incident response plan and Explain legal frameworks and compliance standards	Understanding
CO3	Identify different forensic data acquisition methods	Remembering
CO4	Correlate Windows artifacts with user activity	Analyzing
CO5	Explain network protocols and forensic methodologies.	Understanding
CO6	Explain email header analysis and explain different types of internet artifacts (cookies, cache, history).	Understanding

Course Contents:

Module No.	Detailed Contents	Hrs.	CO No.	Ref No.
1	**Introduction to Cybercrime:** Cyber Crime Attack mode, How are Computers used in Cyber Crimes? Types of Cyber Crime, Cybercrime Statistics in India Prevention of Cybercrime **Introduction to Digital Forensics:** Introduction to Digital Forensics Objective and need of Digital Forensic Types of Digital Forensics Digital Forensic Investigations Process Locard's Exchange Principle, Daubert's Rule **Digital Evidences:** Type , Role of Digital evidence and Rules , sources of Digital Evidences, **Self-Learning topics:** Standards, Guidelines and Best Practices Handling the Digital Crime Scene.	**8**	**CO1**	1,3,7
2	**Incidence Response Process :** Introduction, People Involved in Incident Response Process, Incident Response Process, Incident Response Methodology, Activities in Initial Response, Phases after Detection of an Incident Pre-investigation considerations: The forensic workstation, The response kit, Forensic software, Forensic investigator training, Understanding case information and legal issues, Understanding data acquisition, Chain of custody, Understanding the analysis process, Dates and time zones Hash analysis , File signature analysis, Reporting your findings, Details to include in your report, Document facts and circumstances, The report conclusion. **Self-Learning topics:** CERT	**6**	**CO2**	1,2,5
3	**Data Acquiring and duplication:** Exploring evidence**,** Understanding the forensic examination environment**,** Tool validation**,** Creating sterile media**,** Understanding write blocking**,** Hardware write blocker**,** Software write blocker**,** Rules of Forensic duplication, Defining forensic imaging: DD image, Encase evidence file, SSD device. Imaging tools: FTK Imager, PALADIN **Self-Learning topics:** ENCASE AND FTK Imager	**5**	**CO3**	1,2
4	**Windows Artifact Analysis:** Understanding user profiles, Understanding Windows Registry, Determining account usage, Last login/last password change, **Determining file knowledge**: Exploring the thumb cache, Exploring Microsoft browsers, Determining most recently used/recently used, Looking into the Recycle Bin, Understanding shortcut (LNK) files, Deciphering Jump Lists, Opening shellbags, Understanding prefetch	**8**	**CO4**	2

	Identifying physical locations: Determining time zones, Exploring network history**,** Understanding the WLAN event log**,** Exploring program execution, Determining User Assist**,** Exploring the Shimcache **RAM Memory Forensic Analysis:** Identifying sources of memory, Capturing RAM, Preparing the capturing device, Exploring RAM capture tools, Exploring RAM analyzing tools, Using Bulk Extractor. **Self-Learning topics:** DumpIt, FTK Imager			
5	**Introduction to Network Forensic:** Understanding Password Cracking, Understanding Technical Exploits**,** Analyzing Network Traffic**,** Collecting Network-Based Evidence**,** Evidence Handling**,** Investigating Routers**,** Handling Router Table Manipulation Incidents**,** Using Routers as Response Tools **Mobile Forensics :** Definition, Information available in Mobile Phones, identification, isolation of mobile devices, search and seizure of mobile devices, acquisition methods (physical, logical, file system, JTAG, Chip off), Analysis of mobile images, understanding a mobile forensic report **Self-Learning topics:** Intrusion Detection System its types and Attacks Security features of Mobile Operating System	**8**	**CO5**	1,4 ,10
6	**Email Forensics** – Investigation Techniques, Understanding web-based email, Decoding email, Understanding the email message format, Email attachments, Understanding client-based email analysis, Exploring Microsoft Outlook/Outlook Express, Exploring Microsoft Windows Live Mail, Mozilla Thunderbird Understanding Web Mail analysis, E-mail Investigations Challenge **Internet Artifacts:** Understanding browsers, Exploring Internet Explorer/Microsoft Edge (Old Version),Exploring Firefox, Social media,P2P file sharing, Investigative Report Template, Layout of an Investigative Report, Guidelines for Writing a Report **Self-Learning topics:** Understanding SMTP – Simple Mail Transfer Protocol, Understanding the Post Office Protocol, IMAP – Internet Message Access Protocol	**5**	**CO6**	2

Reference No	Reference Name
1	Digital Forensic by Dr. Nilkashi Jain & Dr. Dhananjay Kalbande
2	Learn Computer Forensic: A beginner's guide to searching, analyzing, and securing digital evidence, William Oettinger Packt Publisher
3	Digital Forensics Basics A Practical Forensic Basic used by Nihad A. Hassan
4	Practical Mobile Forensics, Satish Bommisetty, Rohit Tamma, Heather Mahalik, Packt Publishing Ltd., 2014,ISBN 978-1-78328-831-1
5	Digital Forensics and Incident Response, Gerard Johansen, Packt Publishing
6	Practical Cyber Forensics An Incident-Based Approach to Forensic Investigations Niranjan Reddy, A Press publication
7	Practical Digital Forensics. Forensic Lab Setup, Evidence Analysis, and Structured Investigation Across Windows, Mobile, Browser, HDD and Memory ,A. Bhardwaj, K. Kaushik BPB Publication
8	Practical Windows forensic Packt publisher
9	Practical_Digital_Forensics_Richard_Boddington
10	CHFI Computer Hacking Forensic Investigator The Ultimate Study Guide to Ace the Exam

Web References:

Reference No	Reference Name
1	https://www.rohasnagpal.com/docs/ASCL_Cyber_Crime_Investigation_Manual.pdf
2	https://doi.org/10.6028/NIST.SP.800-86
3	https://onlinecourses.swayam2.ac.in/cec20_lb06/preview

Tutorials:

Sr. No	Topic	Hrs.
1	AI Powered Cyber Crime	1
2	Chain of Custody	1
3	FTK imager and ENCase Imager	1
4	Hashing Tool (md5sum, sha256sum)	1
5	Case Study: Autopsy Tool	1
6	Case Study: To recover deleted files form windows system using Recuva Tool	1
7	Study of SluethKit tool	1
8	Investigation of information of captured packets by using 'Wireshark' tool.	1
9	Extraction of data from an Android device by using the ADB	1
10	Web Browser Forensic using DB Browser for SQLite	1
11	Study of Email Investigation tool	1
12	Guidelines for Writing a Report	1

Assessment:

Continuous Assessment (CA): 25 marks
Following measures can be used for the continuous assessment as:

- Assignments /Quiz /Case studies /Presentations /Projects /Any other measure with the permission of the Director/Principal/HOD/Coordinator.
- The continuous evaluation has to be done throughout the Semester.
- The faculty can use the flexibility of the mode as per the requirement of the course.

Test: 25 marks

- Assessment consists of one class tests of 25 marks.
- The class test is to be conducted when approx. 40 -50% of the syllabus is completed.
- Duration of the class test shall be one hour.

Internal Assessment (IA): 50 marks

- The Internal Assessment marks (out of 50) will be the total of the class test and the continuous assessment.

Term Work: 25 marks

- The term work will be based on the tutorial performance of the student**.**

End Semester Theory Examination:

1. Question paper will comprise of total 05 questions.
2. First question carrying 20 marks and remaining 4 carrying 15 marks each.
3. Total 03 questions (Including first question) need to be solved.
4. Question No: 01 will be compulsory and based on the entire syllabus wherein 4 sub-questions of 5 marks each will be asked.
5. Remaining questions will be randomly selected from all the modules.
6. First question will be compulsory and Students can attempt any two from the remaining four questions.
7. Weightage of each module will be proportional to the number of respective lecture hours as mentioned in the syllabus.